2) разработан и внедрен алгоритм идентификации оператора;
3) получены первые экспериментальные результаты.

Список литературы

1. *Файсханов И. Ф.* Основы управления процессом аутентификации пользователей в социальных и экономических системах : сб. докладов X Международ. конф. «Российские регионы в фокусе перемен». Екатеринбург, 2015. С. 1108–1112.

УДК 004.056

И. А. Шевяков
Научный руководитель: канд. тех. наук, доц. А. Н. Соколов
Южно-Уральский государственный университет, Челябинск

АНАЛИЗ АКТУАЛЬНЫХ УЯЗВИМОСТЕЙ SCADA-СИСТЕМ

Аннотация. В работе рассматриваются актуальные типы уязвимостей программного обеспечения диспетчерского контроля и сбора данных АСУ ТП. Приводится обзор состояния выявления и устранения угроз безопасности АСУ ТП и SCADA-систем в мире, а также основные их типы.

Ключевые слова: защита информации; безопасность АСУ ТП; уязвимость SCADA.

В течение последних десятилетий атаки на АСУТП становятся привлекательной целью, наблюдается значительный рост целенаправленных атак на промышленные информационные системы с целью промышленного шпионажа, мошенничества и нарушения функционирования предприятия. Так, например, на смену отдельным «червям» Stuxnet (2010) и Flame (2012) пришли более изощренные схемы многоступенчатых атак. А для распространения трояна Havex в 2014 г. хакеры взламывали сайты производителей программного обеспечения для управления промышленными предприятиями (SCADA) и заражали официальные дистрибутивы SCADA-систем, которые затем устанавливались на предприятиях, что позволило злоумышленникам получить контроль над системами управления в нескольких европейских странах.

Обзор состояния безопасности АСУ ТП, проведенный компанией Positive Technologies в 2012 г., показал довольно тревожную картину [1, 2]. Резко увеличивается число обнаруженных уязвимостей. С 2010 по 2012 г. установлено в 20 раз больше уязвимостей, чем за предыдущие 5 лет. Каждая пятая уязви-

мость устраняется дольше месяца. 50 % уязвимостей позволяют хакеру запустить выполнение кода. Для 35 % уязвимостей есть эксплойты. Более 40 % доступных в Интернете систем могут взломать хакеры-любители.

Среди всех типов уязвимых компонентов АСУ ТП лидируют SCADA — 87 %, далее следуют системы, обеспечивающие человеко-машинные интерфейсы, — 49 %, реже обнаруживаются уязвимости в программируемых контроллерах — 20 % и совсем редко в используемых протоколах — 1 %.

Самые распространенные типы уязвимостей SCADA-системы:

1) уязвимости аутентификации узлов и данных посредством «слабой» парольной защиты (Authentication). Большая доля таких уязвимостей связана с использованием стандартных инженерных паролей, установленных производителями на приборах промышленной автоматики. Кроме того, пользователи системы часто используют простые, легко запоминаемые пароли, которые могут быть легко определены или, наоборот, сложные для запоминания пароли с их открытым хранением;

2) уязвимости шифрования из-за использования «слабых» криптографических алгоритмов и систем управления ключами (Key Management);

3) уязвимости из-за ошибок конфигурации SCADA-системы (ошибки настройки сетевого оборудования и сетевых служб ОС, ошибки при разграничении прав доступа и полномочий, ошибки при задании разрешений на доступ к ресурсам, применение стандартных шаблонов безопасности и т. п.). Часто производитель системы навязывает неоптимальные политики безопасности либо по умолчанию устанавливает административные права доступа;

4) уязвимости, вызванные отсутствием обновлений безопасности для различных версий SCADA-систем либо несвоевременностью их установки;

5) уязвимости программно-аппаратных компонент, позволяющие использовать DoS-атаки [3] для автоматического выполнения протоколов аварийных или нештатных ситуаций, завершения или «зависания» программ, эксплуатации в системе вредоносного кода. Как правило, такие уязвимости связаны с ошибками программистов — производителей SCADA. Ошибка в программе может позволить злоумышленнику использовать отрытые порты для запуска вредоносного кода в системе, проведения DoS-атаки для переполнения размера буферов данных и т. п.

Распределение уязвимостей SCADA-систем по типам приведено на рис. 1.

Как видно на рисунке, наиболее часто проводятся атаки, использующие уязвимости аутентификации, и атаки, связанные с переполнением буфера программно-аппаратных средств.

За период 2005–2010 г. было обнаружено и устранено 9 уязвимостей SCADA-систем, а после того, как 17 июня 2010 г. была обнаружена троянская программа win32/Stuxnet, резко возрос интерес к системе безопасности АСУ ТП как

со стороны аналитиков информационной безопасности, так и со стороны киберпреступников, итогом такого интереса стало открытие в 2011 г. 64 новых уязвимостей, в 2012 г. — 117, а за 10 месяцев 2013 г. их количество превысило 150. Некоторые производители ПО вплотную занялись устранением уязвимостей своих продуктов. Так, например, фирма Siemens организовала специализированный отдел безопасности SCADA и HMI, задача которого является обнаружение и устранение уязвимостей.

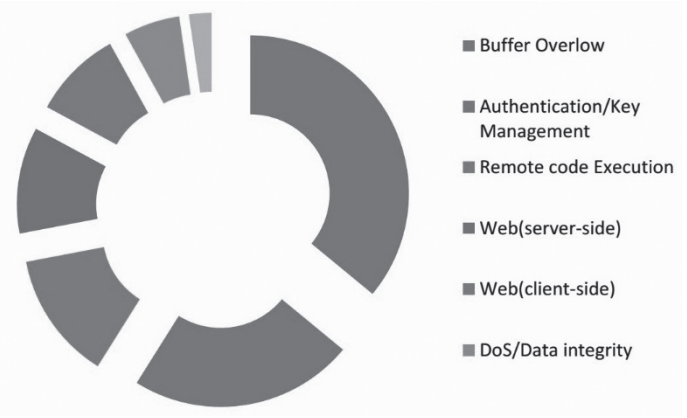

Рис. 1. Распределение уязвимостей по типам

В области защиты систем управления (ControlSystems, SCADA) в настоящий момент существует целый ряд стандартов и рекомендаций [4]. Их можно классифицировать следующим образом:

1) отраслевые решения:
- стандарты NERC для систем управления электрическими сетями;
- стандарты ChemITC для химической индустрии;
- Cisco SAFE for PCN — стандарты Газпрома;

2) рекомендации общего уровня (стандарты NIST, ISA и др.):
- ISA S99 — Комитет общества приборостроения, системотехники и автоматизации (ISA),
- NIST PCSRF Security Capabilities Profile for Industrial Control Systems;
- IEC61784-4;
- КСИИ ФСТЭК.

При этом каких-либо обязательных требований к соответствию определенным критериям безопасности для коммерческих компаний не предъявляется.

На основе вышеизложенного можно сделать вывод, что в большинстве случаев актуальную защиту от проникновения в программное обеспечение АСУ ТП не позволяет выстроить не отсутствие информации о уязвимостях ПО, а отсутствие регламентирующей законодательной базы, носящий обязательный, а не рекомендательный характер. Таким образом существует не-

обходимость применения средств мониторинга функционирования систем диспетчерского контроля и разработка комплекса инженерно-технических и организационных мер, препятствующих реализации хотябы наиболее вероятных сценариев атак.

Список литературы

1. *Пищик Б. Н.* Безопасность АСУ ТП // Вычислительные технологии. Спец. выпуск. 2013. Т. 18. С. 170–175.

2. *Шахновский Г.* Безопасность Систем SCADA и АСУТП. URL: http://www.security-bridge.com/biblioteka/stati_po_bezopasnosti/bezopasnost_sistem_scada_i_asutp (дата обращения: 13.02.2016).

3. *Агафонов А. В.*, *Синадский Н. И.* Тестирование защищенности телекоммуникационного оборудования от сетевых компьютерных атак типа «отказ в обслуживании» с применением генетического алгоритма // Вестн. УрФО. Безопасность в информационной сфере. 2017. № 2 (24). С. 4–9.

4. *Лукацкий А.* Стандарты безопасности АСУ ТП. URL: http://www.slideshare.net/CiscoRu/ss-8690963 (дата обращения: 20.06.13).

УДК 004.056.53

В. В. Шмелёв
Научный руководитель: д-р тех. наук, проф. С. В. Поршнев
Уральский федеральный университет, Екатеринбург

УЯЗВИМОСТИ РАБОЧИХ СТАНЦИЙ И СЕРВЕРОВ

Аннотация. В настоящей статье рассмотрены проблемы уязвимости рабочих станций и серверов. Данное исследование имеет целью выработку рекомендаций, направленных на предотвращение уязвимостей. По сравнению с аналогичными исследованиями, результатами данной работы являются рекомендации, соблюдая которые существенно снижается риск успешной атаки злоумышленников на рабочие станции и сервера.

Ключевые слова: уязвимость; рабочая станция; сервер; пароль; межсетевой экран; администратор; пользователь; обновление.

Значение информации в нашем современном мире можно охарактеризовать известной фразой Натана Ротшильда: «Кто владеет информацией, тот владеет миром». С ростом ценности информации появляется большее количество заинтересованных людей третьих лиц, стремящихся получить несанкциониро-